



DEPARTMENT OF THE NAVY

NAVAL RESERVE READINESS COMMAND REGION TWENTY TWO
BUILDING 2102, NAVAL STATION
EVERETT, WASHINGTON 98207-2600

NAVRESREDCOMREG22INST 5510.2B

N01A

6 May 99

NAVRESREDCOM REG TWO TWO INSTRUCTION 5510.2B

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM

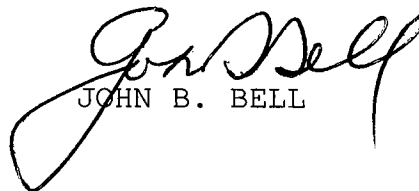
Ref: (a) SECNAVINST 5510.30A
(b) SECNAVINST 5510.36
(c) COMNAVRESFORINST 5500.3A
(d) NAVRESREDCOMREG22INST G5041.1A

1. Purpose. This instruction is provided to supplement the provisions of references (a) and (b). Additionally, it is designed to provide policies and procedures for the management of the Information and Personnel Security Program at this command. Where conflict with directives of higher authority exist, those directives shall take precedence.

2. Cancellation. NAVRESREDCOMREG22INST 5510.2A. This instruction is a complete revision and must be read in its entirety.

3. Applicability. This instruction is applicable to all military and civilian personnel assigned to REDCOM 22.

4. Policy. This instruction establishes policy for the security of classified information and for personnel security matters. Reference (c) provides policy on physical security requirements relating to classified material.


JOHN B. BELL

Distribution:
NAVRESREDCOMREG22INST 5216.1J
LIST A

STOCKED:
NAVRESREDCOM REG TWO TWO (N01A)

TABLE OF CONTENTS

<u>PART</u>	<u>TITLE</u>	<u>PAGE #</u>
	TABLE OF CONTENTS	i
I	PROGRAM MANAGEMENT	I-1
II	SECURITY EDUCATION	II-1
III	SECURITY VIOLATIONS	III-1
IV	CLASSIFICATION MANAGEMENT	IV-1
V	ACCOUNTING AND CONTROL	V-1
VI	STORAGE AND SAFEGUARDING	VI-1
VII	DESTRUCTION	VII-1
VIII	VISITOR CONTROL	VIII-1
IX	PERSONNEL SECURITY	IX-1

APPENDIX

A	EMERGENCY PLAN FOR PROTECTION OF CLASSIFIED MATERIAL	A-1
B	LISTING OF FORMS	B-1

PROGRAM MANAGEMENT
PART I

1. Organization and Responsibilities. Each person who handles classified material, and each office that stores it, is responsible for safeguarding such material. In addition to this general responsibility, the following organizational arrangement and responsibilities exist:

a. Commander. Appoints the Security Manager and ensures effective management of the information and personnel security program.

b. Security Manager. Responsible for and supervises the day-to-day operation of the information and personnel security program. Organizationally, the Security Manager reports to the Commander. This position is governed by the duties in chapter two of references (a) and (b).

c. Assistant Security Manager. Provides policy interpretation and guidance to command personnel and subordinate activities. Ensures positive accounting and control of classified material and provides personnel security services to members of REDCOM 22. The Assistant Security Manager is responsible to conduct Assist Visits and Triennial Inspections of Naval Reserve Activities under the cognizance of the Readiness Command. References (a), (b), and (d) will be utilized in formulating the information security portion of the command inspection program. The Assistant Security Manager reports directly to the Security Manager on all matters pertaining to the information and personnel security program. The Assistant Security Manager is normally a collateral duty of the Director of Command Services and must be filled by an E-6 or above.

d. Security Assistant. Performs technical security duties and maintains accountability programs for secret and NATO material. The Security Assistant reports directly to the Assistant Security Manager on all matters pertaining to the information and personnel security program.

e. Information Systems Security Manager/Officer (ISSM/O). Serves as the point of contact for all command information systems security matters and implements the command information systems security program. This duty is to be performed by the Automated Information Specialist (N6A).

6 May 99

f. Other Organizational Responsibilities. Department Directors retaining classified material are responsible for all classified information stored in their respective areas. Since the most effective step in the protection of classified material is a reduction of the amount of material held, all Departments should reduce classified material whenever possible. This can only be done by destroying material that is no longer considered essential. Only material, which is used frequently, should be retained. All personnel who have access to, or handle classified material, will be familiar with all aspects of handling such material, with emphasis on the contents of chapters four through ten of reference (b).

SECURITY EDUCATION
PART II

1. Security Education. The purpose of security education is to ensure that all military personnel and civilian employees are knowledgeable about classified material and the methods and reasons for protecting it from unauthorized disclosure. The goal is to develop fundamental habits of security to the point that proper discretion is automatically exercised in the discharge of duties and security of classified information becomes a natural element of every task.

a. Orientation briefings will be given to all personnel, civilian and military, who require access to classified information in the performance of their duties. This will normally be done as part of the indoctrination process, or when it is determined that an individual must work with classified information. The Assistant Security Manager is responsible for this procedure.

b. Supervisors are responsible for providing additional on-the-job security training for assigned personnel. This will include personnel who do not hold security clearances to ensure that everyone understands their responsibility to protect classified information. This training may consist of oral reminders to individuals, departmental meetings, or written instructions. The Security Manager/Assistant Security Manager is available to assist.

c. Refresher Briefings. Provided annually to all personnel who are authorized access to classified information. The Security Manager or other professional security sources give this training. It may cover changes to security policy; counterintelligence reminders; stress the continuous evaluation of the information security program; reiterate command procedures for handling, drafting, marking and protecting classified material; detail possible results of compromises due to careless handling of classified information; and various other matters intended to raise the level of security awareness and cooperation of all participating personnel.

d. Counterintelligence Briefing. An agent of the Naval Criminal Investigative Service will give this briefing biennially. Attendance is mandatory for all personnel who have access to classified material secret or above.

6 May 99

e. Indoctrination Briefing. New hire civilians will be indoctrinated within one month of hire. The Assistant Security Manager is responsible for providing this information. All personnel should know, that:

(1) Certain information, essential to the national security, requires protection from disclosure to unauthorized persons;

(2) Classified material will be marked to show the level of classification;

(3) Only those who have been officially and specifically authorized may have access to classified information;

(4) Personnel will be continually evaluated regarding their eligibility to access classified information and to be assigned to a sensitive position.

f. Security Debriefings will be given to individuals, who had access to classified material, prior to termination of military service or civilian appointment, and in certain other instances, per chapter three of reference (a). The Assistant Security Manager will ensure that personnel meeting these conditions receive a debrief and execute a Security Termination Statement (OPNAV 5511/14). The original Security Termination Statement will be placed in the individual's official personnel record for permanent retention.

g. Additional security training will be provided at various intervals on an as-needed basis. This may be in the form of written advisories/notes, or special briefings.

h. Educational security notes will appear in the plan of the month on a routine basis. All personnel are responsible for reading them.

SECURITY VIOLATIONS
PART III

1. There are two types of security violations: one involves a possible or confirmed compromise of classified information; the other involves a failure to adhere to security regulations in situations not involving a compromise.

2. A compromise is the unauthorized disclosure of classified information to a person(s) who does not have a valid clearance, authorized access, or a need-to-know. Compromise is confirmed when conclusive evidence exists that classified information has been disclosed to an unauthorized person. A compromise is possible when circumstances suggest that classified information may have been revealed to a person not authorized access. A possible compromise may also occur when classified information is lost or when classified information was not properly stored or controlled.

a. Reporting Responsibilities.

(1) Any individual who becomes aware that classified information is lost or compromised shall immediately notify the Security Manager, or Staff Duty Officer, if neither the Commander nor Chief Staff Officer are available. If that individual believes that the Commander or Security Manager may be involved in the incident, notify the Commander, Naval Surface Reserve Force (Security Manager). Promptness is important; do not delay reporting because a member of the security team is absent. When a loss or compromise of classified material occurs, the Commander or Security Manager will immediately notify the Naval Criminal Investigative Service (NCIS) Office, Everett. Additionally, the Commander will initiate a Preliminary Inquiry (PI) as required by paragraph 12-4 of reference (b).

(a) Preliminary Inquiry (PI). The Commander, shall appoint, in writing, a command official (other than the Security Manager or anyone involved in the incident) to conduct the PI. The PI shall be initiated and completed within 72 hours. If the PI concludes that a loss or compromise of classified information occurred or a significant command security weakness(es), or vulnerability(ies) is revealed, a PI message or letter will be prepared per paragraphs 12-5 and 12-6 of reference (b) and sent to Commander, Naval Surface Reserve Force, Chief of Naval Operations (N09N2), the originator, the Original Classification

6 May 99

Authority (OCA) of the loss or compromised information, and NCIS, and any other offices specified in reference (b).

(b) Manual of the Judge Advocate General (JAGMAN) Investigation. If the PI concludes that a loss or compromise of classified information occurred or a significant command security weakness(es) or vulnerability(ies) is revealed, the Commander shall initiate a JAGMAN investigation per paragraphs 12-9 through 12-14 of reference (b). The JAGMAN officer shall be appointed in writing. The purpose of the JAGMAN investigation is to provide a more detailed investigation and recommend any corrective or required disciplinary actions. Exhibit 12D of reference (b) is a sample format for a JAGMAN investigation. Whenever serious disciplinary action or prosecution is contemplated against any person(s) believed responsible for the compromise of classified information, formal classification reviews (see paragraph 12-16) of reference (b) shall be coordinated with the Chief of Naval Operations (N09N2), NCIS, and the Office of the Judge Advocate General (Code 11).

(c) Security Review. Classified information subjected to compromise requires a security review for classification determination. The Security Manager will ask the originator of the classified material or the Original Classification Authority to conduct the security review. Personnel assigned to this command shall not declassify properly classified information.

3. Public Media Compromises. A public media compromise is the unofficial release of Department of Defense (DOD) classified and unclassified information to the public resulting in its unauthorized disclosure.

a. Reporting Responsibility. When an individual becomes aware that classified or unclassified information is unofficially released to the public (i.e. newspaper, magazine, book, pamphlet, radio, television broadcast or INTERNET), they shall immediately notify the Security Manager. The Security Manager will comply with paragraph 12-18 of reference (b). No statements or comments, under any circumstances, shall be made concerning any information unofficially released to the public.

4. Other Security Violations. All other security violations, such as open security containers, will also be reported to the

6 May 99

Security Manager. When violations are discovered by watchstanders during evenings, weekends, and holidays, the Staff Duty Officer will be immediately notified. The security container custodians must be recalled to inventory the contents of the security container. While waiting for the custodian, the container will be secured or a watch posted until required action has been completed. The Security Manager will be notified on the first workday following the incident. If the SDO determines that a compromise is likely, the Security Manager and Commander will be promptly notified, and the requirements mentioned in paragraph 2 above will apply.

a. Security Discrepancies Involving Improper Transmission. If the command receives classified information improperly handled, addressed, packaged, transmitted, or transported, a determination by the Security or Assistant Security Manager will be made as to whether the information has been subjected to compromise. If a determination is made that the classified information has been subjected to compromise, the Assistant Security Manager shall immediately notify the forwarding command. Classified information shall be considered as having been subjected to compromise if it has been handled through foreign postal systems, its shipping container has been damaged to an extent where the contents are exposed, or it has been transmitted over unprotected communication circuits. If it is determined that the information was not subjected to compromise, but improperly prepared or transmitted, OPNAV 5511/11 (Security Discrepancy Notice) shall be sent to the forwarding command. All completed Security Discrepancy Notices shall be maintained for two years.

CLASSIFICATION MANAGEMENT
PART IV

1. Classification

a. Information, which requires protection against unauthorized disclosure in the interest of national security, must receive a classification designation. There are three such designations: Top Secret, Secret, and Confidential. Definitions of these terms and guidance on classifying and marking information are found in chapters six through nine of reference (a). All personnel charged with drafting classified material must be familiar with the contents of these chapters.

b. In terms of drafting classified information, it is either "originally classified" or "derivatively classified." REDCOM 22 is not authorized original classification authority, therefore, all classified information drafted by REDCOM 22 personnel will be derivatively classified. That is, the classification of the drafted information will be based upon: Existing documents authored by some activity with original classification authority, a classification guide, an instruction/directive from higher authority. Exhibit 4A of reference (b) lists Original Classification Authority officials. Derivatively classified material will be classified the same as the source material, it cannot be changed except by the originator.

2. Drafting. Drafters of classified documents will comply with chapters four through six of reference (b) in preparing such material. Contact the Security Manager/Assistant Security Manager for assistance. All classified material in draft form will be chopped through the Assistant Security Manager to ensure the correspondence is in the correct format and properly classified. When the document has been signed, the Assistant Security Manager will assign a serial number and date stamp the correspondence.

3. Marking of Classified Information. Classified material will be physically marked, annotated, or identified by other means per chapter six of reference (b). All classified material must be marked in a manner that leaves no doubt about the level of classification and any additional measures necessary to protect the material. Each portion (section, part, paragraph, or subparagraph) will be marked to show its level of

6 May 99

classification, or the fact that it is unclassified. The overall classification will be placed at the top and bottom center of the front cover (if any), the title page (if any), or the first page. The classification of each interior page (except blank pages) will be marked at the top and bottom center of the page. Normally the overall classification of the publication is used.

a. Classified messages are marked at the top and bottom with the overall classification and portion marked per paragraph three above. The first item of text shall be the highest overall classification level of the message. The short form of certain warning notices and all intelligence control markings, shall be spelled out following the message classification level which precedes the message subject line. Copies of messages not electronically transmitted must have the full markings required by chapter six to reference (b).

b. Removable Automatic Data Processing (ADP) storage media and devices (floppy disk, Bernoulli drives, and magnetic tapes) must be labeled using color coded labels (Standard Form 706, 707, 708, or 709) that indicate clearly the classification and associated markings of the information the contain. Mark classified documents produced by AIS equipment per paragraphs 6-33 and 6-34 of reference (b).

recipient. The Security Manager, Assistant Security Manager, or Security Assistant will prepare large distributions, such as instructions, with assistance from the originator.

5. Hand Carrying Classified Material. Hand carrying of classified material is discouraged because of the inherent security risk. Individuals authorized to hand carry classified information or material, either within or outside of the command, must take every precaution to prevent unauthorized disclosure and will adhere to the following:

a. When classified material is being hand carried within the command, the material will be covered using a cover sheet, i.e., Confidential (SF 703), Secret (SF 704) file folder, or whatever covering is needed to protect against casual observation. Double-wrap classified information when hand carrying outside the command. A locked briefcase may serve as the outer cover, except when hand carrying aboard a commercial aircraft.

b. When anyone needs to hand carry classified material to or from the command, the Security Manager must be advised and will brief the individual per the requirements of chapter nine of reference (b) and require such individual to sign a statement acknowledging they received and understood the briefing. If the hand carrying is aboard a commercial aircraft, the provisions of paragraphs 9-11 through 9-13 of reference (b) will be adhered to.

c. Under no circumstances will stops be authorized when hand carrying classified material unless storage at a U.S. Government activity has been arranged.

6. Printing. Classified documents that require printing will be coordinated through the Security Manager prior to processing through the printing coordinator. Arrangements will be made in advance for distribution and storage or print overruns required for future distribution.

7. Inventories. Inventories of Secret material will be coordinated prior to a change of command, upon the relief of the Security Assistant and with the appointment of a new Security Manager, and at least annually.

STORAGE AND SAFEGUARDING
PART VI

1. Storage. Custodial responsibility ranges from the need to cover material on a desk when an unauthorized person approaches, to the requirement that classified material receives a specified type of protection when placed in a security container. Classified material will be stored in General Services Administration approved security containers, Class "A" that meet the standards of chapter ten of reference (b). The Assistant Security Manager will maintain a list of all security containers and is the point of contact for all matters pertaining to security containers.

a. All classified material must be stored in designated containers when not in use and prior to securing for the day. The designated security container for the storage of classified material is located in the Command Services Department. Chapter ten of reference (b) delineates precautions to be taken relative to preliminary drafts, ADP media, typewriter ribbons (one-time), and stenographic notes, worksheets, and all similar items containing classified information.

b. The combination of a security container will be changed whenever any person having knowledge of it has been transferred or no longer requires access; or at any time there is reason to believe it has been compromised. A Security Container Information Form (SF 700) will be used to record combination changes. Part I of the form, containing the names and telephone numbers of individuals to be contacted in an emergency, will be attached to the inside top drawer of the security container. Part II, containing the combination, will be in the classified material control safe at Naval Reserve Center, Everett. These combinations are to be used for emergency access only. If the combination contained in the SF 700 is used for any reason, the Security Manager will be notified the following day so the combination may be changed.

c. The number of people having knowledge of a combination will be limited to those whose official duties demand access to the containers involved.

d. Should it prove necessary to dispose of or transfer custody of a security container, notification of such transaction will be made to the Security Manager. The make,

6 May 99

number of drawers, serial number, and location of the container will be provided. The Security Manager/Assistant Security Manager will ensure no classified material is left in the drawers and reset the combination to 50-25-50. Arrangements will be made with the Logistics Department to excess/dispose of the container.

e. Requirements for new security containers will be referred to the Security Manager who will coordinate the acquisition of the container and set the combination as required.

2. Safeguarding. During working hours, classified material shall be under constant surveillance by an authorized person. Protect preliminary drafts, worksheets, computer printer and typewriter ribbons, computer storage media, and other classified items according to their security classification level. Immediately destroy these items after they have served their purpose. Classified discussions shall not be conducted with or in the presence of unauthorized persons. Files, folders, or groups of documents shall be conspicuously marked to ensure their protection to a degree as high as that of the most highly classified document included therein. Classified document cover sheets may be used for this purpose. Documents separated from the file folder or group shall be marked as prescribed in reference (b). North Atlantic Treaty Organization classified material may be kept in the same container, but it must be kept separately and not mingled with other classified material. Classified document cover sheets, SF 703, and 704 will be used for this purpose; substitute cover sheets are not authorized.

a. Neither money or personal items are to be stored in containers used for classified material. This requirement exists because experience has shown most container break-ins were to steal valuables and not classified material.

b. Working papers include classified notes from a training course or conference, research notes, drafts, and similar items that are not finished documents. Working papers that contain classified information shall be:

(1) Dated when created;

(2) Conspicuously marked "Working Paper" on the first page in letters larger than the text;

(3) Marked centered top and bottom on each page with the highest overall classification level of any information they contain;

(4) Protected per the assigned classification level; and

(5) Destroyed, by authorized means, when no longer needed.

3. Security Checks. A security check will be done each workday by each office that holds and stores classified material.

a. Each security container will have a Security Container Check Sheet (SF 702) posted on the outside. When a container is opened, the date, time, and initials of the individual opening the container will be annotated in the "opened by" column. When a container is secured at the conclusion of the workday, the time and initials of the individual securing the container will be annotated in the "closed by" column. Personnel are to be aware of the requirement for rotating the dial of all combination locks at least four complete turns in the same direction when securing containers.

b. The Staff Duty Petty Officer (SDPO) will check the classified material security container prior to leaving at the end of the workday. This person will ensure that all classified material is put away and the security container is locked, pilferable materials locked in desks or cabinets, lights and appliances turned-off, and doors locked. The individual will sign the SF 702 in the column headed "checked by." This check is required even if the container was not opened that day. In addition to checking security containers, the SDPO will also do random searches to determine whether classified material has been left unprotected. These searches will be confined to offices where security containers are located. An open security container or classified material unprotected constitutes a major security violation. The SDPO will immediately call and advise the Chief Staff Officer (CSO) of the situation. The CSO will recall the custodian to do an inventory. The SDPO will stay at the location of the violation until officially relieved by the SDO. The Security Manager will be notified of the incident as soon as practicable, or on the first workday following the incident.

6 May 99

c. All security violations will be recorded in the Duty Log Book.

4. Disclosure. Classified material will not be disclosed unless disclosure of the information serves a government purpose and adequate security measures are taken to control access to the information and prevent its compromise.

a. Department Heads holding classified material are responsible for ensuring that:

(1) Proper dissemination is made only to cleared personnel on a need-to-know basis.

(2) Any evidence or suspicion of unauthorized disclosure will be reported to the Security Manager.

b. Classified information will not be disclosed over the telephone since normal telephone lines can easily be monitored by unfriendly sources. The only exception to this rule is the use of Secure Telephone Units, Third Generation telephones by personnel trained in their operation.

ACCOUNTING AND CONTROL
PART V

1. Accountability. The Security Manager is responsible for maintaining accountability of all classified material. Departments holding classified material will designate a security coordinator to act as a focal point for the receipt and control of classified material for the department.

2. Receipt. Daily, upon receipt by mailroom personnel, all registered, certified, overnight, express mail, and first class return to sender mail received by REDCOM 22 will be delivered to the Assistant Security Manager or Security Assistant for processing per reference (a). All mail of this type shall be opened the day of receipt due to the possibility of enclosed classified material by personnel cleared to Secret or placed in the Command Services security container until cleared personnel can open, process, and distribute the material. All incoming classified mail will be checked for completeness, violations, or compromise; and if applicable, the originators shall be notified by letter. Records of receipt included with the material will be signed by the Assistant Security Manager and returned to the sender.

a. Confidential/Secret Material. When notified of receipt of confidential and secret material, other than messages, Department Heads will pick-up material from the Assistant Security Manager. Material intended for action/information by more than one department will be acted upon as expeditiously as possible and returned to the Assistant Security Manager for further routing. Secret material will be entered in the REDCOM 22 Information Security Accountability Program, assigned a control number, and put on a NAVRES 5511/5 (Classified Material Control Form). The receiving security coordinator will sign for the document. There will be a continuous chain of receipts for secret material. Procedures for protection of confidential material are less than those for secret. Administrative provisions are required to protect confidential information from unauthorized disclosure and compliance with the regulations on marking, storage, transmission, and destruction. All classified material, including confidential will be stored in the Command Services security container whenever it is not under the constant surveillance of a properly cleared individual.

b. Classified Material Routing. All routing of secret material will be accomplished by the Assistant Security Manager or Security Assistant and will be on a need-to-know basis on a NAVRES 5511/5. Control numbers will be assigned to all secret material. No classified material or document that has been assigned a control number will be transferred to another office without first effecting a change of custody with the Assistant Security Manager. A record of custody change will be maintained until the item is destroyed.

c. Messages. Departments will be routed applicable classified messages as determined by the Security Manager or Assistant Security Manager. Secret messages will be assigned a control number and entered into the Classified Material Control Log. When Secret messages have served their purpose, or when directed by the Security Manager or Assistant Security Manager, they will be destroyed. The Security Assistant will maintain records of destruction for a period of two years. All Secret messages will be maintained in the Command Services Security Container.

3. Reproduction of Classified Material. Reproduction of classified material will be kept to an absolute minimum. Confidential and Secret material will be kept to the minimum number of copies required and must be authorized by the Security Manager or Assistant Security Manager. All classified material that is reproduced will be controlled in the same manner as the original material. Secret material will be entered in the Classified Material Control Log, assigned a control number, placed on a NAVRES 5511/5, and signed for by the Assistant Security Manager. Only the Security Manager, Assistant Security Manager, or Security Assistant will reproduce Secret material and only on certain copying equipment authorized for the reproduction of classified material. Two people will be involved in reproducing classified material to ensure positive control and safeguarding.

4. Mailing/Shipping. The Security Manager, Assistant Security Manager, or Security Assistant, prior to wrapping, will check all classified material mailed/shipped. All transmissions of classified material will follow the guidelines of chapter nine of reference (b). The originating office will double wrap outgoing classified material. Secret material will include a Record of Receipt (OPNAV 5511/10) for execution by the

DESTRUCTION
PART VII

1. Destruction. All destruction of classified material will be accomplished per chapter ten of reference (b). The first week in January is designated as classified information "clean-out" week in which specific attention and effort are focused on disposition of unneeded classified and controlled unclassified information.

a. Although no longer required by reference (b), two individuals having a security clearance at least as high as the category of material being destroyed will accomplish the destruction of secret material. These personnel shall be thoroughly familiar with chapter ten of reference (b). Under normal circumstances, classified material will be destroyed utilizing the shredder cleared for destruction of classified material located in the mail room. A record of destruction is required for Top Secret material, but not for Top Secret classified waste, Secret or Confidential material. Although not required by reference (b), destruction of Secret material will be recorded in Section IV of NAVRES 5511/5 (or an OPNAV 5511/12 (Classified Material Destruction Report). The original of NAVRES 5511/5 or the OPNAV 5511/12 is placed in the Classified Material Control Log and a copy retained by the custodian. The record of destruction is to be retained for two years.

b. Destruction may be accomplished by using an appropriate shredder, or by any other means approved in chapter ten of reference (b) for the media being destroyed. The method used to destroy classified material must prevent later recognition or reconstruction. The Security Manager/Assistant Security Manager will provide assistance in determining the proper method of destruction and assist in the destruction process if necessary.

VISITOR CONTROL
PART VIII

1. Visitor Control. The term "visitor," as used for security purposes, is any person who is not attached to or employed by REDCOM 22. The term "visitor" also includes personnel on temporary additional duty, personnel on temporary duty orders, or those personnel assigned on a quota to schools involving a classified course of instruction.

a. When a visit to a DON command will involve access to classified information, the commanding officer of the visitor or an appropriate official of the contractor facility, or organization will submit a visit request either by Naval message or command/company letterhead to this command. Visit requests must include the following information for military and civilian personnel:

(1) Full name, rank, rate, or grade (when applicable), date and place of birth, social security number, title, position, UIC/RUIC (when applicable), and citizenship of the proposed visitor.

(2) Name of employer or sponsor, if other than the originator of the request.

(3) Name and address of the activity to be visited, if other than the addressee of the visit request.

(4) Date and duration of the proposed visit.

(5) Purpose of the visit in detail, including estimated degree of access required. When the visit involves access to information, such as NATO or SIOP-ESI, for which specific authorization is required, the command visited will confirm that the visitor has been briefed and authorized such access.

(6) Security clearance status of visitor (basis of clearance is not required).

b. Verification of contractor visits will be accomplished per paragraph 11-2.3 of reference (a).

c. Per paragraph 11-2.4 of reference (b), formal visit requests are not required for personnel within the Region who are U.S. citizens with whom working relationships have been established. When there is an established working relationship and the clearance level and bounds of need to know of the employee are known, a visit request is not necessary.

d. Visit requests may be received and sent by facsimile, by message, or electronically transmitted via electronic mail. When transmitted by facsimile, the visit request must be on official letterhead.

e. Under no circumstances will personnel hand carry their own visit requests to the place being visited. Under no circumstances will REDCOM 22 allow access to classified information to personnel not mentioned in paragraph 1c above who hand carry their visit request without verification from the member's parent command.

f. For more detailed information concerning visit requests of non-DOD personnel, foreign nationals, and members of Congress, refer to chapter 11 of reference (a).

g. Each Department will ensure that the following guidelines are observed when visitors are in their areas:

(1) Visitors must have proper identification and have been cleared by the Security Manager, Assistant Security Manager, or Security Assistant to have access to classified material;

(2) Be aware of all visitors in the department and do not have classified material where it can be unnecessarily viewed;

(3) Do not openly discuss classified material.

h. Meetings in which classified information will be discussed audibly, must be approved in advance by the Security Manager.

6 May 99

PERSONNEL SECURITY
PART IX

1. Security Clearances

a. A personnel security clearance is an administrative determination that an individual is eligible, from a security standpoint, for access to classified information of the same or lower level as the clearance granted. When issued, a certificate of clearance does not in itself constitute authority for access to classified information. It is a determination of eligibility for access. Disclosure of classified information is controlled by the access authorized to an individual and then only when the need-to-know is clearly established.

b. Newly assigned personnel, military and civilian, must have their clearance and access status reinstated if assigned duties that require access to classified material. When it is necessary to request reinstatement, the following procedures apply:

(1) Determine if the clearance requested is absolutely required on a strict need-to-know basis.

(2) The Security Assistant will initiate requests for personnel security clearances on personnel assigned, using the Personnel Security Action Request (OPNAV 5510/413). No permanent clearance will be granted without final approval from the Department of the Navy Central Adjudication Facility for that level of clearance. Temporary clearances may be granted for periods up to six months only if there is evidence that the member has an investigation approved for the level of temporary clearance, or a completed National Agency Check/Single Scope Background Investigation has been mailed to the Defense Investigative Service. Security clearances will be granted at a level consistent with need-to-know, and the access will be granted on the same basis.

3. Access

a. As discussed in paragraph 1a of this section, possession of a security clearance does not constitute access. Access is based on the need-to-know. Authorizing access is a

separate and distinct matter from that of granting a security clearance. The ultimate authority for controlling access rests with the Security Manager.

b. Access to classified information will be authorized and controlled using OPNAV 5520/20. The Security Manager is authorized to act upon and grant access for personnel assigned who meet the eligibility criteria of reference (a).

4. Continuous Evaluation of Eligibility. Each individual's eligibility for access to classified information will be continuously evaluated. Any potentially significant information, which could place in question an individual's loyalty, reliability, or trustworthiness, and any significant personnel security factors found in chapter ten of reference (a) will be reported to the Security Manager. Changes in an individual's behavior, mental or emotional illness, hostile and foreign connections, subversive activity, alcohol or drug abuse, or security violations are items that might cause questioning and must be reported. Commands should act to identify individuals with personal problems at an early stage and to guide them to programs designed to counsel and assist them.

a. All members of the command, particularly those in legal, medical, and supervisory positions, must report to the Security Manager all unfavorable information which is obtained or developed and which fall into the categories listed in chapter ten of reference (a) such as:

- (1) Criminal conduct
- (2) Apparent mental, emotional or personality disorder(s)
- (3) Unexplained affluence or excessive indebtedness, etc.

b. Co-workers have an equal obligation to advise their supervisors or the Security Manager when they become aware of information with potential serious security significance regarding someone with access to classified information.

c. Supervisors will comment on the eligibility of personnel for continued access to classified information and discharge of security responsibilities with regularly scheduled performance

appraisals of military and civilian personnel whose duties requires access to classified information.

d. On an annual basis, the Security Manager will provide a listing of all personnel who have access to classified information. This listing will be reviewed by Department Heads and returned indicating any changes desired.

5. The personnel security policy and procedures described in this section are based upon and governed by reference (a). The Security Manger/Assistant Security Manger will strictly comply with this instruction to ensure a high level of integrity exists for the protection of classified material.

EMERGENCY PLAN FOR PROTECTION OF CLASSIFIED MATERIAL
APPENDIX A

1. Background. Each command, which handles classified material, is required to develop an emergency plan for the protection of classified material in case of a natural disaster, civil disturbance, or other emergency situation. This appendix is REDCOM 22's Emergency Plan. It is required reading for all personnel who handle classified material. The Security Manager is charged with keeping the plan current and providing adequate educational guidance to ensure staff members are knowledgeable of emergency procedures when activated.

2. Purpose. To provide instructions for handling classified material during emergency situations.

3. Action. There are three types of emergency situations: natural disaster, civil disturbance, and emergency action (e.g., fire, bomb threat) that require additional actions to ensure protection of classified material. These additional actions are: guarding the material, removing the material, or complete destruction of the material.

a. The Commander or the Security Manager (during their absence, the SDO) will implement the emergency plan for evacuation/destruction of classified material.

b. Upon determination that any emergency exists or is imminent, one of the above officials will authorize any or all of the following actions:

(1) Remove all classified material from desks and working spaces and lock it in the appropriate security container.

(2) Secure the area in which classified material is stored.

(3) Transfer all classified material to the Administrative Office to be placed in the command designated security container.

(4) Request security assistance from Naval Station Everett.

(5) Implement emergency destruction.

c. Natural Disaster. Most natural disasters occur without warning. However, every effort must be made to at least lock-up classified material. After the danger has passed, an inventory will be completed.

d. Civil Disturbance. The Commander, Chief Staff Officer, or Security Manager will determine whether classified material should remain secured in work spaces, concentrated at one central location (e.g., Command Services Department Office), or destroyed.

(1) Should the first alternative be directed, classified material will be locked in the Command Services Department classified material security container and a copy of the inventory list kept in a separate location. Every effort should be made to remove any signs, which would indicate where classified material is stored.

(2) Should the second alternative be directed, the procedures in subparagraph 3b(3) above will be followed.

(3) Should emergency destruction be directed, the following procedures are prescribed:

(a) Classified material will be destroyed using the shredder certified for the destruction of classified material located in the Mail Room, or burned in metal trash cans. If the base is not invaded, burning may be done outdoors. If intruders are on the base, burning should be done in the heads or near water sources.

(b) Priority for destruction: Secret first, then confidential; for official use only material will be destroyed if time permits. Every attempt should be made to record what material checking off the inventory list destroys.

e. Emergency Action. The Security Manager or Chief Staff Officer will determine and direct appropriate action in any other emergency condition.

(1) Fire. Secure classified material in the Command Services Department security container or in another lockable container if time permits. Ensure office is vacated. Shut (do not lock) door and exit the building via the most expeditious route. Do not use the elevators, as they may lose power. The saving of life is the paramount consideration.

(2) Bomb Threat. Follow search procedures contained in reference (b). If the building must be evacuated, follow the same procedures as for fire.

(3) Detection of Entry/Theft in Progress. Notify the Staff Duty Officer and the Security Manager if classified material appears to have been compromised. Attempt to impede entry or theft if appropriate to circumstances. Do not use force in the process except to prevent injury or death.

(4) After-the-Fact Detection of Entry or Theft. If evidence of tampering with classified material exists, notify the Staff Duty Officer and Security Manager.

f. In the event of fire, bomb threat, or any emergency condition requiring firefighting personnel or other persons not cleared for access to classified material to be used for removal of classified material from the security container, these persons will be briefed/debriefed per reference (a) and requested to sign a briefing/debriefing statement.

LIST OF FORMS
APPENDIX B

1. Forms

a. The following forms can be obtained from the navy stock system:

<u>FORM/STOCK NUMBER</u>	<u>DESCRIPTION</u>
OPNAV 5511/10 NSN 0107-LF-008-8000	Record of Receipt
OPNAV 5511/12 NSN 0107-LF-010-0500	Classified Material Destruction Report
OPNAV 5511/13 NSN 0107-LF-055-1165	Record of Disclosure
OPNAV 5511/14 NSN 0107-LF-055-1171	Security Termination Statement
OPNAV 5521/27 NSN 0107-LF-055-2235	Visit Request
SF 700 NSN 7540-01-214-5372	Security Container Information
SF 701 NSN 7540-01-213-7899	Activity Security Checklist
SF 702 NSN 7540-01-213-7900	Security Container Check Sheet
SF 703 NSN 7540-01-213-7903	Cover Sheet (Confidential)
SF 704 NSN 7540-01-213-7902	Cover Sheet (Secret)
SF 707 NSN 7540-01-207-5537	Secret ADP Label
SF 708 NSN 7540-01-207-5538	Confidential ADP Label

NAVRESREDCOMREG22INST 5510.2B
6 May 99

FORM/STOCK NUMBER

DESCRIPTION

SF 710
NSN 0080-00-007-0100

Sensitive Unclassified ADP Label

a. The NAVRES 5511/5 (Classified Material Control Form) and NAVRES 5511/6 (Classified Material Access Certification) are computer generated forms.